Service Oriented Acquisition: Harmonizing Horizontal Requirements with a Traditionally Vertical Process

Chris Gunderson
NPS, JITC & W2COG
Chris.Gunderson@w2cog.org

Abstract

The Department of Defense has adopted the concept of Netcentric Operations and Warfare, i.e. .effective, distributed, collaboration over a network to gain asymmetric advantage, especially with respect to information superiority. To enable NCO/W, the DoD has issued transformational policy mandating change from a vertical (stovepiped), serial, system-centric requirement model to a horizontal, capability-based, adaptive, requirement model. This policy specifically calls for using the service oriented architecture (SOA) paradigm as a change agent, and a means to accelerate delivery of information processing capability. However, the intent of this SOA-enabled netcentric requirements policy is at odds with the implementation detail mandated by Acquisition policy. That is, Acquisition policy does not offer tools to enable, let alone encourage, cross program development of enterprise capability or to de-couple software development from the rigid, serial, time-lines associated with developing sensors, weapons, and platforms. This paper suggests a way to subtly nudge two aspects of the existing policy regime to provide those tools. In particular, the Net-Ready Key Performance Parameter (NR-KPP) should be based on a minimal matrix of measurable and testable criteria that can be observed on the ground, written into enforceable contract language, and rolled up into executive dashboards. The Tailored Information Support Plan (T-ISP) concept should be expanded to include the notion of a network service stack (NSS) to address enterprise-level information processing capability.. The intent of a NSS T-ISP would be to provide a plan, enforceable through contract language, that will maintain NR-KPP service level objectives throughout a capability lifecycle.

1. A service oriented paradigm for IT interoperability testing: Net-Ready Assessment.

The Department of Defense has issued policy explaining its desire to become a "netcentric" [1] enterprise enabled by a Global Information Grid (GIG). To enforce this policy in the DoD Acquisition process, DoD has created the "Net-Ready Key Performance Parameter (NR-KPP). Traditionally, KPP's are rigid, mandatory, engineering specifications associated with major DoD programs. The NR-KPP is intended to ensure that artifacts fielded on the GIG contribute and conform to the objectives of a netcentric enterprise. "Netcentric" implies an adaptive and collaborative approach to information processing, a concept at odds with the traditional rigidity of KPPs. Hence, net-ready assessment, i.e. validation and verification (V&V), test and evaluation (T&E), and/or certification and accreditation (C&A) of "net-readiness", should be an adaptive and collaborative process. Adaptive and collaborative assessment is a profoundly new concept for DoD. Net-ready assessment should therefore not be hidebound to the bureaucracy of the status quo. Rather, net-ready assessment should be a useful engineering service embedded throughout the software development and deployment process, based on measurable and testable parameters that will accomplish the following:

> Reduce Acquisition policy and requirements documents into measurable and testable attributes that can be coded in machine readable formats for testing and used as the basis for contract enforcement language.
>
> Decrease the time and money developers spend on testing by consolidating various aspects of testing (e.g. C&A, Interoperability), sharing best practices across programs, and standardizing assessment methods across certification authorities.
>
> Focus assessment on software architecture rather than software build, so that "most current COTS/GOTS component" can be a test criteria.
>
> Bundle candidate information processing capabilities into reference implementations of

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
21 MAY 2008	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Service Oriented Acquisition: Harmonizing Horizontal Requirements with a Traditionally Vertical Process	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Joint Interoperability Test Command**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
AFCEA-GMU C4I Center Symposium "Critical Issues In C4I" 20-21 May 2008, George Mason University, Fairfax, Virginia Campus, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**27**	

net-ready architecture that can be tested independently for compliance, and then used as a universally validated component instead of testing thousands of services for compliance with hundreds of often vague standards.

Assess both adequacy of service oriented infrastructure (e.g. enterprise security and semantic interoperability) and value added to business objectives (i.e. targeted improvements in mission outcomes.)

Weigh risk and reward to scale the rigor of assessment as appropriate to address the spectrum from small and/or generic COTS or GOTS software modules (e.g. Google Earth) to large and/or specialized "systems" (e.g. Future Combat System.)

Assist developers of large complex systems to deploy their capability continuously and incrementally as a "system of services" composed largely of COTS and GOTS modules.

Rapidly assess information processing capability prior to its operational deployment by heavily leveraging modeling and simulation. Follow up with operational V&V that holds developers responsible for delivering targeted service levels of mission performance improvements.

Create an on-line digital feedback loop to capture lessons learned and assist in the tasks described above.

Reduce the barrier to entry for IT vendors and developers that don't traditionally support the DoD by hiding the complexity of DoD policy and process behind recognizable, comfortable, e-market interfaces.

1.1 Net-ready assessment's three broad categories.

1.1.1 Do no harm (assurance and performance).

The GIG will be a network of interactive software and hardware services that propagate and evolve quickly and without central control, *by design*. This federated design requires discipline across the federation to ensure that a candidate new service does not negatively impact the existing ecosystem. Net-ready assessment should address software assurance (SwA) with respect to how the assessed software architecture affects overall network vulnerability, latency, lifecycle cost, and reliability.[2] Current methods for testing SwA are immature, and although the net-ready assessment process will deliberately evaluate and incrementally improve those methods, they will never be perfect. Therefore, the task is to manage risk rather than eliminate it. Some risk and/or service degradation is acceptable if tradeoffs warrant. For example it may be acceptable to gain higher assurance at the cost of greater latency, more functionality at the cost of lower reliability, or greater speed to better capability at the risk of introducing some vulnerability. Operational customers will be the final arbiter of the acceptability of these tradeoffs during operational V&V.

1.1.2 Bind to *Trustworthy* Service Oriented Architecture (SOA) infrastructure (reusable and composable).

"Bind-ability," i.e. the ability to quickly compose new capability from distributed components, is a key aspect of netcentricity. SOA is a technological approach that can be used to compose capability (i.e. "mash up") across a network. (The idea of "composability" applies to both on-line operational use of the capability, and engineering re-use of the technology.) "Enterprise Service Bus" (ESB) is a generic term used in industry to represent the interfaces, protocols, and objects that form the framework for a particular SOA. We can define SOA IA infrastructure as enterprise IA services plus the ESB (or other framework) that governs their use. If an SOA *IA* infrastructure achieves DIACAP (Defense Information Assurance Certification and Accreditation Process) certification, it will have been deemed "trustworthy" to the level of assurance associated with its C&A. (Note that the IA infrastructure for any particular network operation includes more than SOA IA infrastructure. DIACAP accreditation of operational environments will include traditional vulnerability assessment of basic IA infrastructure that includes things like firewalls, packet sniffers, encryption, and physical security. Certainly nothing about SOA mitigates vulnerabilities imbedded in applications deployed on local computing platforms. However, it is possible and useful to decouple consideration of the vulnerability associated with SOA activity governed by an ESB or other SOA framework.) Consequently we can "compose" trustworthy information operations by binding various Community of Interest (COI) services to the trustworthy infrastructure and invoking enterprise IA services each time data is exchanged. By metering the ESB, we can assess data transactions that occur from a particular COI service across the ESB. If all assessed transactions invoke IA services properly we can (1) "certify" the data

transactions as "assured", and (2) assess the associated COI service as "net ready" to deploy in any similarly configured trustworthy SOA infrastructure.

The elements that define a "service" in a SOA designed for composability (e.g. Web-SOA) are: (a) self-describing; (b) discoverable; (c) executable via open standard interfaces. Assessing those elements requires a test environment that provides a realistic representation, i.e. a "reference implementation," of the target SOA infrastructure.

Per NSA's GIG IA policy [3], key elements that define "IA services" are: (a) developed by the U.S. Government at high assurance levels defined by the "Common Criteria"; (b) *authenticate* identity of people and machines that join the network including their current level of access and mission role; (b) *authorize* access to data and services according to dynamic modular policy that governs Risk-adaptive Access Control (*RAdAC*); (c) provide Multi-Level Security (*MLS*); (d) audit all data transactions that occur on the network. *Reference implementations* composed of combinations of these IA services, properly governed by an ESB, or other SOA IA Infrastructure, will be certified and accredited via DIACAP.

Components of trustworthy SOA infrastructure will be incrementally improved, tested, and fielded to increasingly automate a process that dynamically authorizes or denies access to data and services on the basis of identity, current role, and emergent operational conditions. The level of certified and accredited assurance, i.e. the degree of trustworthiness, of a SOA infrastructure will increase as IA services and governing IA framework are incrementally improved, validated, and verified.

The test of whether or not a candidate net-ready artifact is self described, discoverable, and executable via open standards is to require that artifact to bind effectively with a reference implementation of certified trustworthy SOA infrastructure. When a tested software component binds to a trustworthy SOA infrastructure, data transactions that include interaction with that component can be trusted to the level of the SOA IA Infrastructure's accreditation, by definition Hence, the tested artifact need not "come with" or establish its own IA accreditation. Rather, through duly diligent SwA assessment per paragraph 2. a., and by demonstrating ability to conduct trusted transactions across an ESB (or similar framework), a component can be certified as net-ready to deploy across any similarly accredited trusted SOA infrastructure.

1.1.3 Add value.

Candidate artifact should actually demonstrate improved capability. Accordingly, testers and developers should work with operational customers to define objective, testable, measures of effectiveness (MOEs) based on objective mission performance improvement goals. Testable MOEs might include mission planning cycle time reduction, "kill chain" compression, reduction of the amount of inventory at rest in a supply chain, etc. The operational customer will be the final arbiter of the acceptability of objectively demonstrated service levels during an objective operational audit of the deployed capability.

1.2. Net-ready attributes.

DoD NR-KPP Policy [4] describes four "pillars" of the NR-KPP, the Netcentric Operations and Warfare Reference Model (NCO/W RM), IA Policy, Enterprise Architectural Framework, and Key Interface Profiles (KIPS). With respect to information processing across an Internet Protocol network, the four pillars can be summarized as a requirement to demonstrate and document operational value added via IA, SOA, and data strategy.

A useful definition of "netcentric value added" is "enables rapid ad hoc discovery and collaborative application of distributed capability to achieve an asymmetric advantage." Note that interoperability is a necessary, but not sufficient condition for netcentricity. Netcentric = Discoverable + Interoperable + Collaborative + Effective

Netcentric value added applies to engineering, acquisition, logistics, and training as much as it does to operations. All these disciplines should collaboratively enable asymmetric advantage with respect to mission outcome and acquisition efficiency.

Hence, a net-ready assessment must perform rapid, adaptive, and collaborative V&V with respect to IA, SOA, and data strategy. It should employ objective MOEs in context with operations, engineering, acquisition, logistics, and training. Assessment should include due diligence in pre-deployment simulations and verification in post deployment operational scenarios. Per discussion above, and as summarized in Figure 1, the netcentric performance attributes are as follows:

> "Discoverable" means that data, services and technology can be easily found and used by previously unassociated entities. Collaboration among unknown providers and consumers of data, services and technology *requires a pragmatic strategy to put data, services and technology in context*

with critical conditions of interest. Producers must create and register metadata with respect to content, context and administrative detail. Consumers must create and register their critical conditions of interest. Data owners must define dynamic discretionary access policy rules that describe objective criteria for weighing the need to protect vs. the need to share information. An agreed *intellectual property rights (IPR) model must support discovery and re-use of useful, information, services, and technology and information.*

"Interoperable" means that a *capability will bind with another previously unknown capability usefully and ad hoc*. Therefore interoperability requires use of open standard interfaces. However, compliance with any contemporary set of software "standards" does not guarantee interoperability; reference implementation is required. Note that capability must be deployable under an intellectual property rights (IPR) model that supports binding with other modules.

"Collaborative" means that information value is enhanced as a result of interaction. It takes energy to interact with unfamiliar entities. Merely enabling exchange of bits among disparate players does not enhance productivity. (E.g., providing unlimited email access to soldiers in a hot zone is unlikely to enhance productivity.) Effective netcentric collaboration requires a disciplined approach to ensuring a high value-per-bit-of-data-exchanged ratio. *Testers will assist developers and customers define critical conditions of interest, and discretionary access rules, for the anticipated family of information exchanges*. The assessment process can thereby inform communities that share critical conditions of interest and help them develop pragmatic semantic strategies for productive collaboration.

"Effective" means objectively demonstrated value added. The artifact must enable information to be shared more usefully. The net-ready assessment will include a post deployment operational audit to verify that a tested artifact actually improves service levels with respect to objective MOE. Delivering more bits is not the goal; the goal is to *deliver more value per bit*. Value added can be operational, engineering, and/or acquisition. Any latencies, unreliability, or vulnerabilities must be offset by benefits. Any useful capability developed by the government should be reusable.

Traditionally, network architectural views focus on the OSI "link" layer of data bit exchange. Web services make it practical to conduct information exchange without concern for the detail of the bit flow. It is this more abstract information exchange architecture that facilitates netcentricity. So, in an netcentric, i.e. service oriented, architecture the DoD Architectural Framework (*DODAF) views should be represented at or above the OSI "session" layer*. Further, the "system view" in an SOA should represent a "service view."[5]

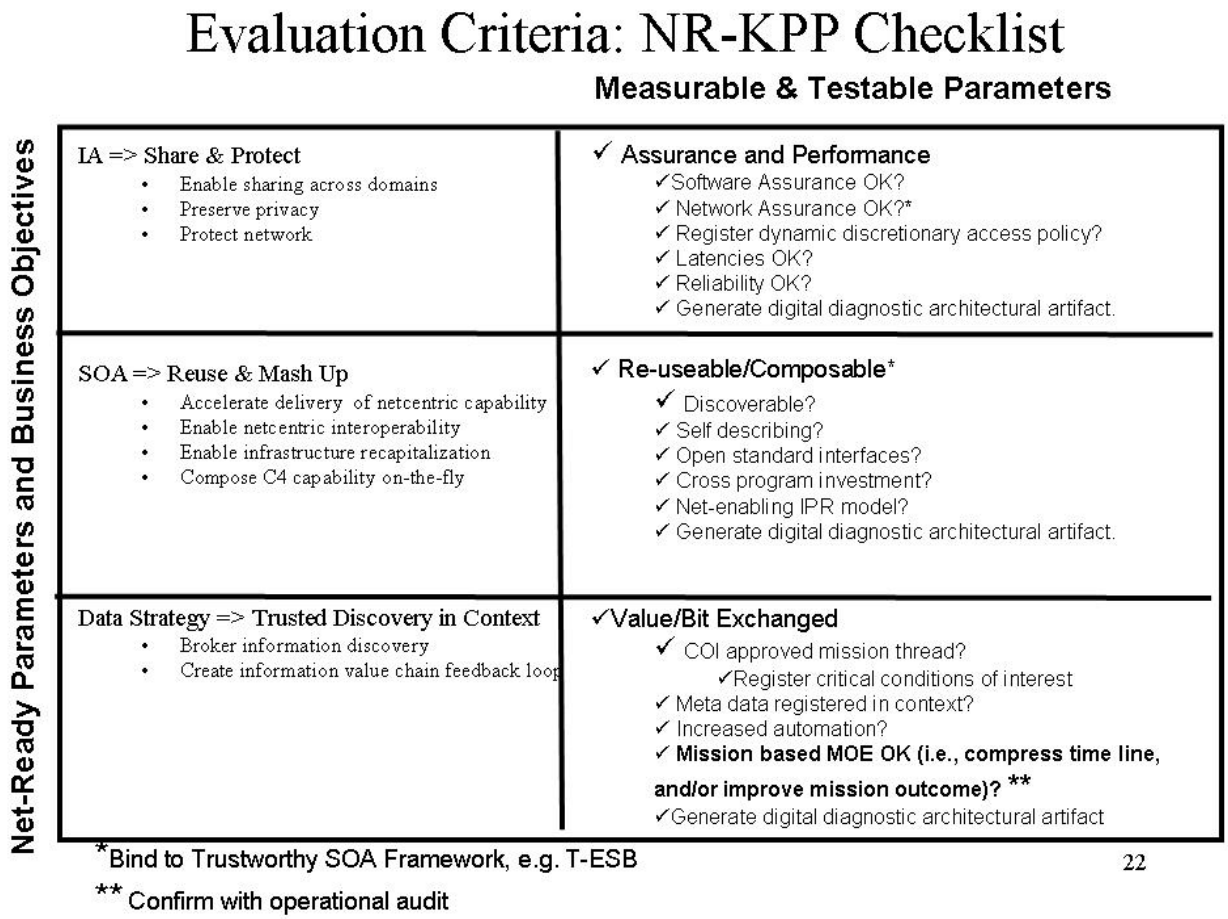


Figure 1: NR-KPP Assessment Matrix

Artifacts should be assessed as modules in an enterprise rather than as stand alone systems. If a module is net-ready it will be expected to interact across multiple programs, and therefore across multiple supporting requirements, (e.g. JCIDS), acquisition (e.g. DoDI 5000.2), and DODAF documents.) It doesn't make sense to force a one-to-one relationship between an *enterprise* capability and a particular program. *The net-ready assessment process will therefore map tested capability modules to capability requirements in support of multiple programs.*

The net-ready assessment should be largely *runtime activity and minimize paperwork.* As discussed in reference (e), the mere existence of architectural design artifacts, e.g. DoDAF view, does not guarantee, or even imply, netcentricity. *A net-ready assessment will demonstrate that a capability module actually does interact netcentrically with the other components of a SOA infrastructure* and thereby feed the net-ready software standard development process. Rather than require pre-created *prognostic* DODAF views, the net-ready assessment will use mission simulations to *diagnose* the actual netcentric architectural functionality. The operational "view" (OV) will illustrate the collection of simulated operational information exchanges, i.e. the mission threads. The technical view (TV) will illustrate the collection of invoked interfaces. The system (or service) view (SV) will illustrate the collection of invoked service interactions. In a web SOA all these interactions occur at or above the OSI session level, and can be observed at the OSI application layer. Hence, web tools can generate graphic representations of these different netcentric architectural abstractions as necessary for net-ready assessment documentation as a by product of, rather than a requirement for, testing. Any *paper documentation required should be automatically generated as a by product of demonstrated capability, not as a pre-condition to the test.*

The NR-KPP assessment matrix (figures 2-4) provides objective assessment guidance per discussion above. The net-ready assessment process will automate, streamline, and share best practices to

help developers map their artifacts to the NR-KPP assessment matrix.

NR-KPP Assessment Matrix

Criteria	Assessment Criteria		
	IA	SOA	Data Strategy
Documentation			
Submit Netcentric Service Stack TISP Request	N/A	Provide NSS TISP	N/A
Register mission models.(s) to be used for V&V. (Submit modeling language (e.g. BPEL) mission model(s) and mission level objectives (MLO); Identify SLAs; identify operational sponsor(s) and COIs.)			Register sponsor(s), COIs, scenario(s), MOE, SLAs,and use cases
Describe net-ready strategy	Provide C&A roadmap	Provide SV-4B	Provide data strategy
Describe re-used GFE netcentric architectural components	ID assured components (NCES or certified alternative)	ID GFE SOA	ID Meta-Data registry
What is the existing software maturity and functionality pedigree? (CMI maturity model or similar? Consumer report? Developer's internal process?)	ID C&A status	ID software architecture pedigree (CMMI, standard stack, code print, etc)	N/A
Is the intellectual property rights (IPR) model compatible with netcentric reusability? (Register all IP license agreements. Determine whether IPR issues may help or hinder reuse from both operational and engineering perspective)	N/A	Register IPR model	N/A
Illustrate the netcentric architecture invoked by information exchanges demonstrated during runtime simulations. (Configure the suite of services. Execute mission simulations. Generate DoDAF views as necessary.)	N/A	Generate diagnostic OV5, SV4b, TV in runtime	N/A

Figure 2: Proposes NR-KPP Assessment Matrix Assessment Criteria

NR-KPP Assessment Matrix

Criteria	Assessment Criteria		
NETCENTRIC Functionality (SOA Functionality)			
Assurance and Performance	**Test for S/W assurance and performance**	**Test for network assurance and performance**	**Test for semantic interoperability**
Does the assessed artifact impact reliability? MOE = % of time operational	N/A	Reliability in simulation =?	N/A
Does the assessed artifact impact (+ or - transactional latency? MOE = time per information transaction	N/A	Transaction latency in simulation=?	N/A
Does the assessed artifact introduce IA vulnerability? MOE = S/W Assurance Vulnerability score; % of time service denied; # unintended disclosers; PL #? Does assessed artifact perform adequately w/rt industry best-of-breed?	S/W Assurance vulnerability score? S/W Performance score?	Assured transactions across ESB or similar framework accredited at PL =? Network downtime in simulation =?	Disclosures in simulation?
Does lifecycle model address re-capitalization via tech refresht? MOE = COTS currency	N/A	Current build? Yes/no?	N/A
Is the artifact discoverable? Is artifact self described and employ open interfaces? MOE = yes/no GIG SOA reference model	Does artifact discover + bind to IA services?	Does capability module map to current commercial standard SOA RM (e.g. OMG, OASIS, etc)? Does artifact discover + bind to Trusted SOA in run time? Does trusted SOA services discover and bind to artifact in run time?	Is metadata registered for content, context, and admin? Does artifact auto-register new metadata? What percent of on line data is discoverable in context?

Figure: 3 Proposed NR-KPP Assessment Criteria

NR-KPP Assessment Matrix

Criteria	Assessment Criteria		
Value Added	**Test for dynamic accesses control**	**Test for operational and/or engineering reusability**	**Test for value per bit exchanged**
Is the artifact sponsored by multiple operational activities and/or cost codes? MOE = # of sponsors; %$ leveraged against other programs	N/A	# of sponsors =? % dollars mutually leveraged = ?	# of COI members contributing to ontology growth
Does IPR model encourage re-use? MOE = cost of enterprise license; open source development model yes/no?	Are intellectual property rights protected?	$/seat = ? Open source?	N/A
Does life cycle model increase relative percentage of resources available for tech refresh and retiring legacy capability vs. sustainment? MOE = % $ for re-capitalization	N/A	% Contract cost for retiring legacy % Contract cost for tech refresh % Contract cost for sustaining legacy	NA
Does the artifact enhance value per bit exchanged? I.e., does the artifact achieve "mission level objectives" (MLO)? MOE = time; # of cycles; casualties, probability of kill, units of issue, etc; yes/no	Are dynamic rules to address authorization re: need to know vs. need to share registered?	Are operational mission threads, MOES and service levels registered? (E.g., Speed to better decision? # of planning cycles per day? Kill chain duration? Inventory at rest? Time in training pipeline?)	Are critical conditions of interest (CCI) registered? Does simulation indicate MLO's achieved?
OPTEST	SLA's achieved? Is operational community satisfied with service levels delivered?	SLA's achieved? Is operational community satisfied with service levels delivered?	MLA's achieved? Is operational community satisfied with service levels delivered?

Figure: 4 Proposed NR-KPP Assessment Criteria

2. A service oriented paradigm for IT network integration and life cycle support: Network Service Stack Tailored Integration Support Plan (NSS T-ISP).

2.1 The issue is a "horizontal" information-centric requirement addressed by a vertical system-centric acquisition model.

DoD policy for Acquiring, integrating, and maintaining capability on the Global Information Grid mandates addressing supportability and cross-program interoperability early in the development process via an "Information Support Plan" (ISP)[6], and emphasizes an intent to leverage Commercial Off the Shelf (COTS) software; employ rapid incremental development techniques; re-use successful engineering components across programs.[7] This policy acknowledges that acquiring information processing capability should be handled differently than acquiring platforms, sensors, or weapons. Nevertheless, the policy enforcing directives invoke the formal requirements process across the full acquisition spectrum. They cite the need for formal artifacts, in addition to ISP, such as Joint Capability Integrated Design System (JCIDS) Analysis of Alternatives (AoA) documents, Integrated Capability Document (ICD), Capability Design Document (CDD), and Capability Planning Documents (CPD). These artifacts are expensive and take years to generate. They typically govern large "systems" funded by single "vertical" domain sponsors.

Other DoD policy [8][9][10][11][12][13] mandates service oriented architecture (SOA), information assurance, and data interoperability to enable "Netcentric Operations and Warfare" (NCO/W). This policy requires network software infrastructure that can be shared across programs in both build time and run time. It describes how the SOA paradigm can be used to achieve that objective faster, better and cheaper than previous approaches to interoperability through agile, continuous, improvement to network enabled capability. For example, typical SOA-enabled COTS software builds are delivered annually with quarterly updates. This rapid, incremental software development cycle can support AoA, Engineering Design Modeling (EDM), Development, or Life Cycle Maintenance (LCM), as

defined in DoD Acquisition policy, equally well. Further, many information processing requirements are identical across programs and SOA theoretically makes it easy to share, re-use, and/or improve software components developed by others.

Clearly, DoD specifically intends to apply the inherent modularity and composability of SOA to support its Acquisition objectives. However, JCIDS AoA, ISP, ICD, CDD, and CPD, are typically vertical (i.e. describing specialized systems), monolithic (i.e. a lot of money and time spent to deliver quantum improvement in capability), and serial (i.e. non-iterative progression from developing formal requirements, through engineering milestones, to deployment, through life cycle support.) Hence these artifacts, designed to field major systems, are at odds with the SOA approach to deploying information processing capability, i.e. horizontal (i.e. generic flat infrastructure), incremental (i.e. capabilities deployed rapidly in small pieces with options to try alternative vectors), and parallel (i.e. iterative continuous feedback among requirements, engineering, deploying, and lifecycle support).

In fact, these directives call for Test and Evaluation Master Plans (TEMPS) that proceed from Development Testing (DT), to Operational Testing (OT), to Interoperability Testing (IOT), to Certification and Accreditation (C&A). In this model, software is tested in the same serial fashion as platforms, weapons, or sensors. For example, a program's software build is frozen at DT until it undergoes OT at least eighteen months later. This approach guarantees that software will be out of date by the time a system is deployed. Further, there is no standard Acquisition artifact that enables, let alone encourages, managers from different programs to mutually develop requirements, find investment partners, or identify existing solutions.

The Deputy Undersecretary of Defense for Acquisition, Technology and Logistics (DUSD AT&L) recognizes a need for less onerous approach, and has created an option for a *Tailored* Information Support Plan (T-ISP).[14] The T-ISP allows small programs, legacy systems, and/or rapid technology insertion projects to develop and demonstrate supportability and cross-program interoperability with minimal supporting documentation. However, T-ISP is still program-centric and system-centric. It does not provide a means for programs (large or small) to leverage SOA as a means to deliver or consume shared network capability.

A Joint Staff Instruction [15]defines the Net-Ready Key Performance Parameter (NR-KPP). It explains that NR-KPP should address network IA, SOA-enablement, data strategy, and mission enhancement in parallel, and that NR-KPP assessment should begin early in the development cycle. JITC is developing a process and measurable and testable criteria toward those ends. If the NR-KPP defines the necessary and sufficient criteria for supportability, interoperability, and security; then it follows that an ISP should simply be a roadmap to achieve, demonstrate, and maintain NR-KPP compliance. A tailored TEMP (T-TEMP) could facilitate the process by using early and continuing NR-KPP assessment to validate that a particular software *architecture* is net-ready. In that case there would be no need to freeze a program's software *build*. DT, OT, IOT, and C&A would simply test and evaluate the deploying system with the current build of its software architecture installed.

Many leaders in DoD recognize the issues and opportunities described above. Accordingly, they have chartered various projects aimed to create federated development and test and evaluation (D, T&E) platforms. DISA in fact is working toward two variants of a Federated Development and Certification Environment (FDCE). The idea is that resources like FDCE would provide a means for autonomous domains to conveniently and effectively collaborate, especially with respect to network enabled, and network enabling software.

2.2 The solution is to create a complementary "horizontal" information-centric process servicing the verticals.

To bridge the gap between the stated need for cross program collaboration and the lack of an enabling process, DoD should make a subtle adjustment to an existing tool. That is, DoD should add a new eligibility category for T-ISP. Call this category "Network Service Stack" (NSS) to be cited in lieu of "program" or "system" on the current T-ISP standard documentation. Define NSS to include software services, framework, resources and/or applications associated with a well defined, service architecture. Use the T-ISP process to continuously collect, document, and advertise successful "SOA reference implementations" of network service stacks. Use these certified SOA reference implementations as test artifacts.

DoD should adopt the net-ready assessment criteria outlined in figures 1- 4 as the basis for defining the NR-KPP for any particular capability. Define NSS T-ISP as "a roadmap for designing, refining, and complying with a tailored NR-KPP assessment matrix for a given network service architecture." Define an NSS that is successfully assessed against NR-KPP criteria as "architecturally net-ready". Define a Tailored TEMP (T-TEMP) to ensure that the current build of the net-ready software

architecture is assessed during DT, OT, IOT, and C&A of deploying systems. In other words, T-TEMP will both enable and require government program managers to consume "architecturally net-ready" COTS and GOTS software at the same rate it is updated.

NSS T-ISP-eligibility (currently ACAT II, II, & Non-ACAT) should expand to include the SOA-enabled information processing aspects of ACAT I programs. Federated D, T&E platforms (e.g. FDCE) can serve as resources to develop and execute NSS T-ISPs. In this way, software engineering gets decoupled from the slower moving aspects of system development, and major programs can perform agile, incremental, software engineering (AoA, EDM, production, and life cycle maintenance) on COTS-like time scales. Further, program managers can conveniently leverage each others' investments in information processing infrastructure.

Vendors should pay a fee for service to use the NSS T-ISP process and get "pre-approval" for their architecturally net-ready NSS COTS offerings. This will help government program managers to more readily leverage COTS software for AoA, EDM, development, and life cycle maintenance.

The beauty of this service-oriented approach to analysis of alternatives is that it can be applied to validate itself. DoD can quickly learn if it works by investing in a handful of short duration, low cost pilot projects spirals designed around well known requirements for network services that provide assured Quality of Service for things like security, privacy, and priority delivery of valued information.

[1] Net-Centric Operations and Warfare (NCOW) Reference Model (RM) (https://disain.disa.mil/ncow.html)
[2] OMG Software Assurance Ecosystem
[3] Information Assurance (IA) Component of the Global Information Grid (GIG) Integrated Architecture
[4] CJCS 6212.01, 8 Mar 2006, Interoperability and Supportability of information Technology and National Security Systems
[5] DoD Architectural Framework (DoDAF) v 1.5
[6][6] DODI 4630.8, 30 June 2004, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)
[7] DODI 5000.2, 12 May 2003, Operation of the Defense Acquisition System
[8] Information Assurance (IA) Component of the Global Information Grid
[9] CJCS 6212.01, 8 Mar 2006, Interoperability and Supportability of Information Technology and National Security Systems
[10] Net-Centric Operations and Warfare (NCOW) Reference Model (RM) (https://disain.disa.mil/ncow.html)
[11] Netcentric Check List (NCCL)
[12] DODD 8320.02, 2 December 2004, "Data Sharing in a Net-Centric Department of Defense."
[13] DoD Architectural Framework version 1.5
[14] ASD NII Memorandum, "Information Support Plan (ISP) Acquisition Streamlining Pilot Program Tailored," 26 August 2005
[15] CJCS 6212.01, 8 Mar 2006, Interoperability and Supportability of information Technology and National Security Systems

World Wide Consortium for the Grid (W2COG) Institute: *Assured* Value-of-Information-Service (V*oIS) across a networked enterprise*

"ACQUISTION LITE": Better networked capability - faster, and cheaper - through adaptive collaborative, value-focused, architecture, engineering, and acquisition

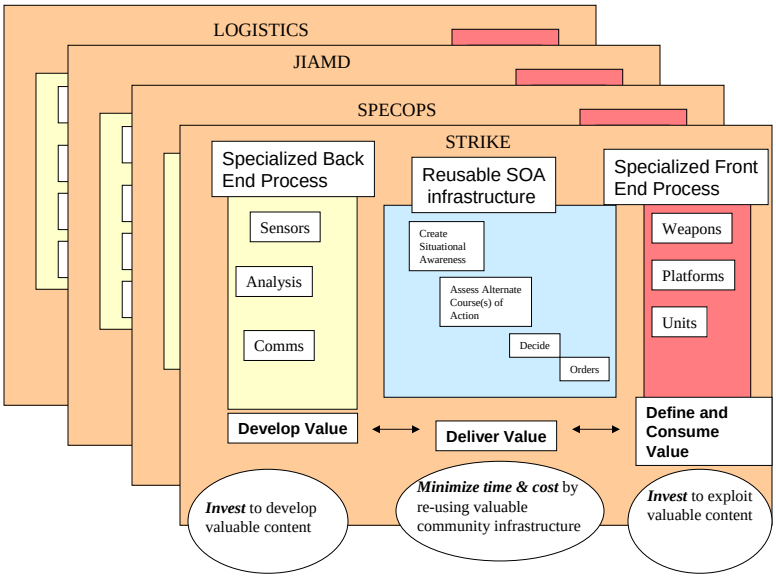
Chris.Gunderson@W2COG.org
(o) 703 262 5332
(m) 831 224 5182
www.w2cog.org

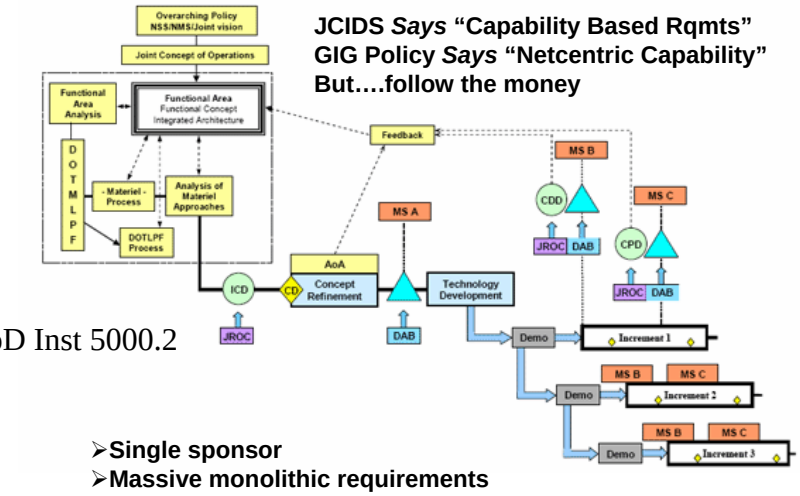
Observations

- COTS software in government systems is generally out of date at IOC and falls farther behind throughout life cycle.
- Government requirements process does not intercept new COTS s/w vectors or sunset archaic s/w requirements.
- Government rapid technology insertion methods use COTS as gap fillers that generally lack sustainment tails.
- IRT the above, enlightened *e-Gov* policy *mandates* COTS, SOA, OSS, and "best" industrial practice (e.g., "Adopt, Buy, Create", FDCE, AOpen Technology Development, etc.)

➢ ***e-Biz unwritten "policy" is to <u>leverage competition</u> in the marketplace…***

GIG “Netcentric” SOA Value Proposition is to reuse and continually improve shared computer network infrastructure





JCIDS *Says* “Capability Based Rqmts”
GIG Policy *Says* “Netcentric Capability”
But….follow the money

DoD Inst 5000.2

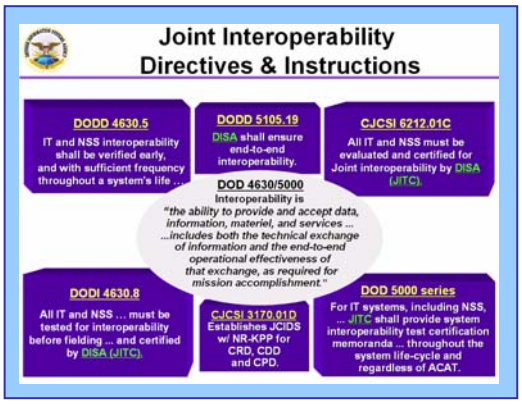
- **Single sponsor**
- **Massive monolithic requirements**
- **Expensive, repetitive, paper documentation**
- **Long serial process**

Program IOC ~ 10 years

Challenge & Opportunity: Business as Usual or e-Biz?

"Net-Ready-KPP" (NR-KPP)/ NR-KPP Cert …*Develop)*
…Verifiable performance measures …to assess information needs…"

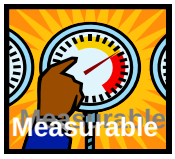
"…The Tailored Information Support Plan (T-ISP) is intended to accelerate the certification process…"



Joint Interoperability Test Command (JITC) directed to enforce the T-ISP and NR-KPP… → **JCIDS/ACQ Lite**

Net-Ready Key Performance Parameter (NR-KPP) + Tailored Information Support Plan (T-ISP): a *netcentric accelerant co-evolved by government and industry operators, developers, and testers* ….. not a show stopper or rubber stamp … ***H&R Block not the IRS!***

NR-KPP = •Semantic Data Strategy •Geospatial SOA Framework •Enterprise Security **+** ***NETCENTRIC VALUE ADDED!** (Acquisition & OPS!)* **=** ✓Dynamic Multi-Level Privacy ✓Streamlined Supply Chain ✓Better Decisions Faster



T-ISP = **JCIDS-lite** **+** **ACQ-lite** **=** ✓Parallel iterative JCIDS/ACQ ✓Dynamic on-line documents ✓Quarterly capability increments → *

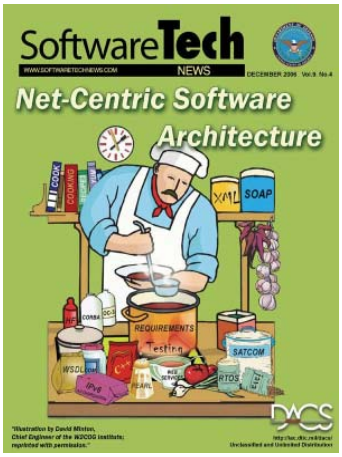
•Tighter OODA Loop
•Increased interaction among coalition
•Decreased inventory at rest
•Faster speed to market
•Shortened training pipeline
•Improved test scores
•Fewer casualties
•Decreased maintenance down time
•Etc …

W2COG Institute

International, collaborative of network technology and operations experts from government and industry

Capability Brokering service to put expert providers in touch with consumers

- www.GIGlite.org **Process model** for Open Technology Development of network infrastructure:
  - Distributed build-time development
  - Distributed run-time T&E
  - Adaptive collaborative V&V
  - "Open" intellectual property regime
  - Library of certified net-ready reference implementations



GIG To-Be Acquisition Vision

Innovators' "dating service" to broker customers and providers of net-enabling products and services

NR-KPP based Consumer Report format that compares bundles of similar net-enabling products and services

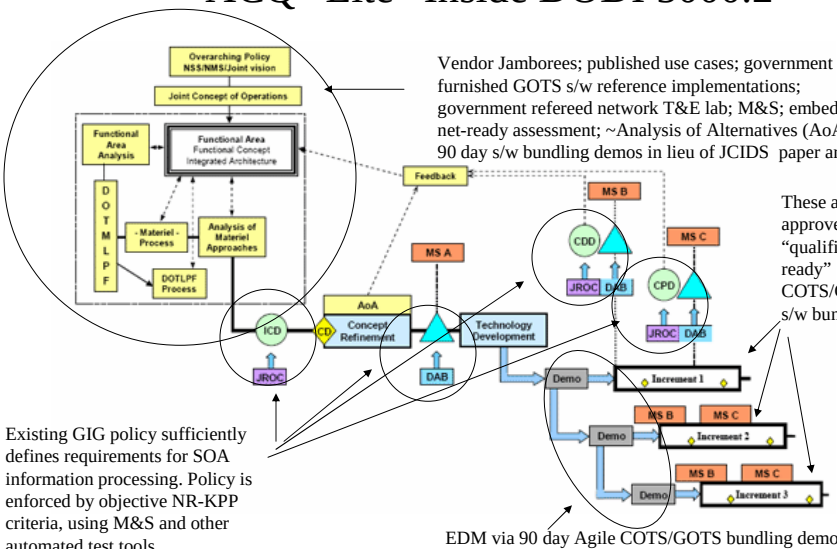
Net-Ready e-Portal

Consumable COTS & GOTS bundles *certified* to deliver netcentric increments of Valuable Information at the Right Time (VIRT) via trusted information transactions, i.e. Value Off the Shelf (VOTS)

"GIG-lite"
- On-line SOA DEVNET
- Secure multi-level access
- Dynamic Library:
  - Netcentric RQMTS
  - Mission Threads
  - Mission Level Models
  - VOTS S/W offerings

Commercial e-Market offering certified bundles of net-enabling products and services

ACQ "Lite" Inside DODI 5000.2



Vendor Jamborees; published use cases; government furnished GOTS s/w reference implementations; government refereed network T&E lab; M&S; embedded net-ready assessment; ~Analysis of Alternatives (AoA) via 90 day s/w bundling demos in lieu of JCIDS paper artifacts

These are pre-approved "qualified net-ready" COTS/GOTS s/w bundles

Existing GIG policy sufficiently defines requirements for SOA information processing. Policy is enforced by objective NR-KPP criteria, using M&S and other automated test tools

EDM via 90 day Agile COTS/GOTS bundling demos, or "sprints". These can be used as down selects or simply net-ready qualifying opportunities

GFE COTS/GOTS software build every ~ 360 days

Program IOC ~ 10 years

Evaluation Criteria: NR-KPP Checklist

Measurable & Testable Parameters

Net-Ready Parameters and Business Objectives

IA => Share & Protect • Enable sharing across domains • Preserve privacy • Protect network	✓ Assurance and Performance ✓Software Assurance OK? ✓ Network Assurance OK?* ✓ Register dynamic discretionary access policy? ✓ Latencies OK? ✓ Reliability OK? ✓ Generate digital diagnostic architectural artifact.
SOA => Reuse & Mash Up • Accelerate delivery of netcentric capability • Enable netcentric interoperability • Enable infrastructure recapitalization • Compose C4 capability on-the-fly	✓ Re-useable/Composable* ✓ Discoverable? ✓ Self describing? ✓ Open standard interfaces? ✓ Cross program investment? ✓ Net-enabling IPR model? ✓ Generate digital diagnostic architectural artifact.
Data Strategy => Trusted Discovery in Context • Broker information discovery • Create information value chain feedback loop	✓Value/Bit Exchanged ✓ COI approved mission thread? ✓Register critical conditions of interest ✓ Meta data registered in context? ✓ Increased automation? ✓ **Mission based MOE OK (i.e., compress time line, and/or improve mission outcome)? **** ✓Generate digital diagnostic architectural artifact

*Bind to Trustworthy SOA Framework, e.g. T-ESB

** Confirm with operational audit

Acquisition Lite Artifacts

Process	Directive	Capability Broker Deliverable
JCIDS	CJCSI 3170.01, DODI 4630.8	Tailored ISP
FAR/DFAR	DODI 5000 series	DODINST 5000.2 compliant artifacts, e.g. BAA, RFI, RFP, Source Selection Plan, Risk Mitigation Plan, SOA COTS Acquisition Strategy, Contract SLAs
IA Compliance, e.g. DIACAP	DODI 8500 series	Enterprise "Type Accreditation" (Trusted SOA DIACAP certification plan)
NR-KPP= (NCOW = IA+ SOA+ Data Strategy) + KIPS + DoDAF	CJCSINST 6212.01, NCO/W Ref Model, KIPS, NSA GIG IA policy, DoDAF v1.5	Measurable and Testable Net-Ready Parameters, diagnostic DoDAF views
T&E	DODI 5010.4, 4630.8	Tailored TEMP (latest COTS GFE is tested at DT and goes to OT)

- Back Up

NR-KPP Assessment Matrix

Criteria	Assessment Criteria		
	IA	**SOA**	**Data Strategy**
Documentation			
Submit Netcentric Service Stack TISP Request	N/A	Provide NSS TISP	N/A
Register mission models.(s) to be used for V&V. (Submit modeling language (e.g. BPEL) mission model(s) and mission level objectives (MLO); Identify SLAs; identify operational sponsor(s) and COIs.)			Register sponsor(s), COIs, scenario(s), MOE, SLAs,and use cases
Describe net-ready strategy	Provide C&A roadmap	Provide SV-4B	Provide data strategy
Describe re-used GFE netcentric architectural components	ID assured components (NCES or certified alternative)	ID GFE SOA	ID Meta-Data registry
What is the existing software maturity and functionality pedigree? (CMI maturity model or similar? Consumer report? Developer's internal process?)	ID C&A status	ID software architecture pedigree (CMMI, standard stack, code print, etc)	N/A
Is the intellectual property rights (IPR) model compatible with netcentric reusability? (Register all IP license agreements. Determine whether IPR issues may help or hinder reuse from both operational and engineering perspective)	N/A	Register IPR model	N/A
Illustrate the netcentric architecture invoked by information exchanges demonstrated during runtime simulations. (Configure the suite of services. Execute mission simulations. Generate DoDAF views as necessary.)	N/A	Generate diagnostic OV5, SV4b, TV in runtime	N/A

NR-KPP Assessment Matrix

Criteria	Assessment Criteria		
NETCENTRIC Functionality (SOA Functionality)			
Assurance and Performance	**Test for S/W assurance and performance**	**Test for network assurance and performance**	**Test for semantic interoperability**
Does the assessed artifact impact reliability? MOE = % of time operational	N/A	Reliability in simulation =?	N/A
Does the assessed artifact impact (+ or - transactional latency? MOE = time per information transaction	N/A	Transaction latency in simulation=?	N/A
Does the assessed artifact introduce IA vulnerability? MOE = S/W Assurance Vulnerability score; % of time service denied; # unintended disclosers; PL #? Does assessed artifact perform adequately w/rt industry best-of-breed?	S/W Assurance vulnerability score? S/W Performance score?	Assured transactions across ESB or similar framework accredited at PL =? Network downtime in simulation =?	Disclosures in simulation?
Does lifecycle model address re-capitalization via tech refresht? MOE = COTS currency	N/A	Current build? Yes/no?	N/A
Is the artifact discoverable? Is artifact self described and employ open interfaces? MOE = yes/no GIG SOA reference model	Does artifact discover + bind to IA services?	Does capability module map to current commercial standard SOA RM (e.g. OMG, OASIS, etc)? Does artifact discover + bind to Trusted SOA in run time? Does trusted SOA services discover and bind to artifact in run time?	Is metadata registered for content, context, and admin? Does artifact auto-register new metadata? What percent of on line data is discoverable in context?

NR-KPP Assessment Matrix

Criteria	Assessment Criteria		
Value Added	**Test for dynamic accesses control**	**Test for operational and/or engineering reusability**	**Test for value per bit exchanged**
Is the artifact sponsored by multiple operational activities and/or cost codes? MOE = # of sponsors; %$ leveraged against other programs	N/A	# of sponsors =? % dollars mutually leveraged = ?	# of COI members contributing to ontology growth
Does IPR model encourage re-use? MOE = cost of enterprise license; open source development model yes/no?	Are intellectual property rights protected?	$/seat = ? Open source?	N/A
Does life cycle model increase relative percentage of resources available for tech refresh and retiring legacy capability vs. sustainment? MOE = % $ for re-capitalization	N/A	% Contract cost for retiring legacy % Contract cost for tech refresh % Contract cost for sustaining legacy	NA
Does the artifact enhance value per bit exchanged? I.e., does the artifact achieve "mission level objectives" (MLO)? MOE = time; # of cycles; casualties, probability of kill, units of issue, etc; yes/no	Are dynamic rules to address authorization re: need to know vs. need to share registered?	Are operational mission threads, MOES and service levels registered? (E.g., Speed to better decision? # of planning cycles per day? Kill chain duration? Inventory at rest? Time in training pipeline?)	Are critical conditions of interest (CCI) registered? Does simulation indicate MLO's achieved?
OPTEST	SLA's achieved? Is operational community satisfied with service levels delivered?	SLA's achieved? Is operational community satisfied with service levels delivered?	MLA's achieved? Is operational community satisfied with service levels delivered?

Proposed *JCIDS-LITE* PROCESS

•Requirements are defined as executable mission models

•FAA, FNA, FSA, PIA are parallel, non-sequential and iterative rather than serial

• Documentation is on-line "living" digital artifacts rather than static

• Artifacts are hosted in on-line dynamic, run-time, repository and test & evaluation environment (GIG-Lite)

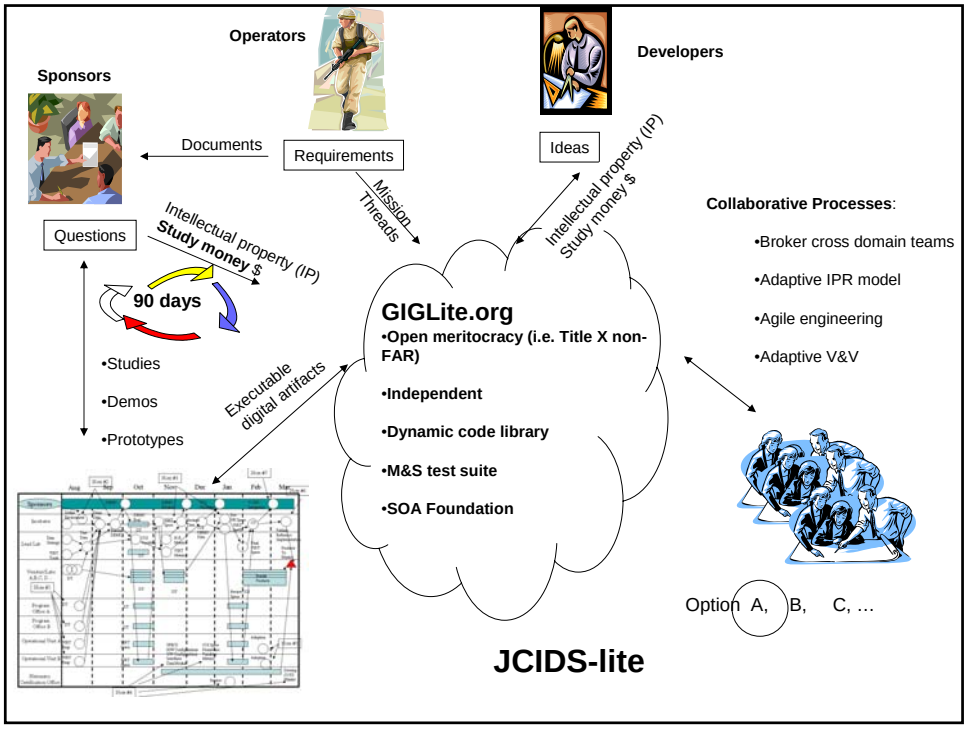
Proposed DOD 5000.X *Acquisition Lite*

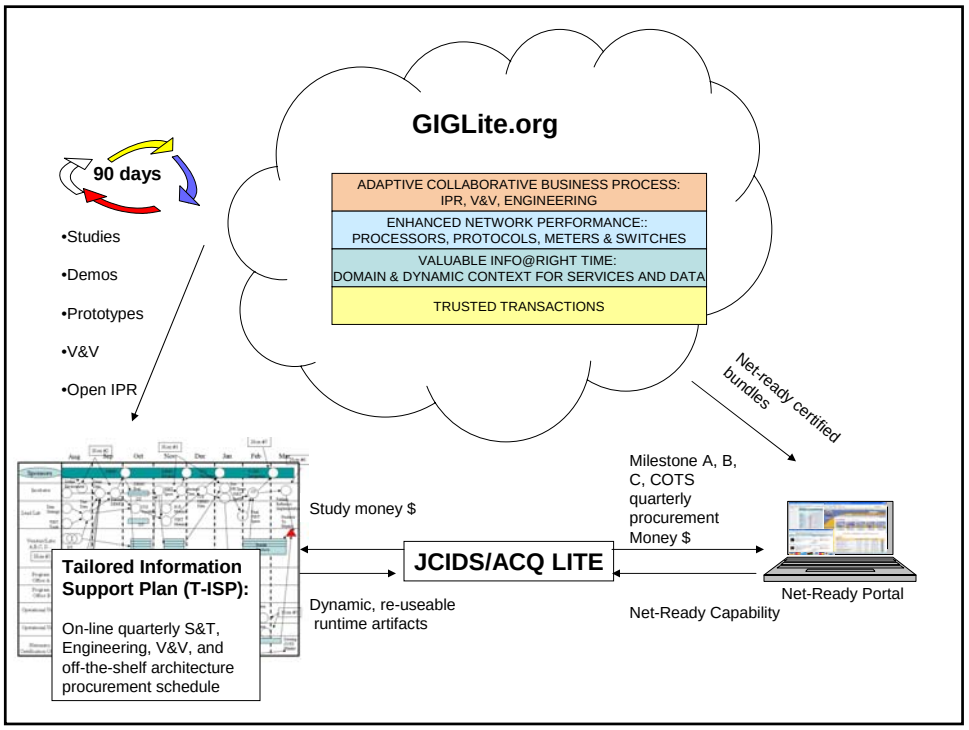
- Milestones are iterative, parallel, and interactive with JCIDS
- Architecture focuses on information processing requirement not technology stack
- Mission model based validation and verification (V&V) is embedded with software development and is adaptive, and collaborative
- Software development includes quarterly off-the-shelf procurement spirals
- GIG-lite.org serves as dynamic repository of "living" digital artifacts

NR-KPP + T-ISP = JCIDS/DoD 5000 Acquisition "lite" for GIG Information Processing Components

JCIDS/ACQ Lite requires a public/private partnership designed to accelerate a "net-ready" market for products and services that facilitate *trusted transactions of valuable information at the right time:*

- A "Dot org" facilitates rapid non-FAR information processing discovery cycles via ***"open" IPR model*** and self selecting industry-academic-government project teams
- A light weight "Dot gov" administration office manages a ***distributed major software "test range"*** that brokers adaptive, distributed, net-ready V&V, and facilitates transfer of funds, artifacts, and intellectual property across government community of sponsors, operators, and labs
- Standing ***Title 10 compliant, but non-FAR legal vehicle between .org and .mil*** streamlines non-proprietary, capability-based, T&E & discovery process for all participants
- On-line ***"GIGLite.org"*** serves as dynamic run-time repository of requirements, capabilities, best practices/practitioners, and lessons learned
- JCIDS/ACQ ***documents (e.g. JCD, ISP, CDD,CPD, NR-KPP) become "living" parallel & iterative on-line digital artifacts*** that continuously capture and propagate new requirements, discoveries, policies, and best practices
- Bundles of off-the-shelf DOTMLTF capability, are certified as net-ready, visible, consumable and continuously deployed via ***commercial e-Portal***

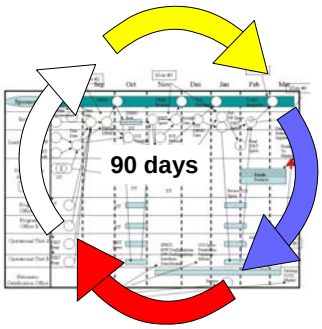

Operators
Developers
Sponsors
Documents
Requirements
Ideas
Intellectual property (IP)
Study money $
Mission Threads
Questions
90 days
•Studies
•Demos
•Prototypes
Executable digital artifacts
GIGLite.org
•Open meritocracy (i.e. Title X non-FAR)
•Independent
•Dynamic code library
•M&S test suite
•SOA Foundation
Collaborative Processes:
•Broker cross domain teams
•Adaptive IPR model
•Agile engineering
•Adaptive V&V
Option A, B, C, …
JCIDS-lite


GIGLite.org
90 days
•Studies
•Demos
•Prototypes
•V&V
•Open IPR
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
ENHANCED NETWORK PERFORMANCE:: PROCESSORS, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS
Net-ready certified bundles
Tailored Information Support Plan (T-ISP):
On-line quarterly S&T, Engineering, V&V, and off-the-shelf architecture procurement schedule
Study money $
Dynamic, re-useable runtime artifacts
JCIDS/ACQ LITE
Milestone A, B, C, COTS quarterly procurement Money $
Net-Ready Capability
Net-Ready Portal

GIG: OPS

ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS

T-ISP: Pooled Gov't & Industry JCIDS study money and Intellectual Property



T-ISP: Milestone A, B, C, D, and life-cycle maintenance quarterly off-the-shelf procurement

JCIDS/ACQ Lite
Objective is to continuously populate the GIG with increments of re-useable information processing capability validated and verified in GIGLite.org

Program A | MS A | MS B | MS C | FOC | Maintenance

GIGLite.org : M&S

ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS

0 | 1yr | 2yr | 3yr | 4yr | 5yr | 6yr | 7yr

GIG

ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS

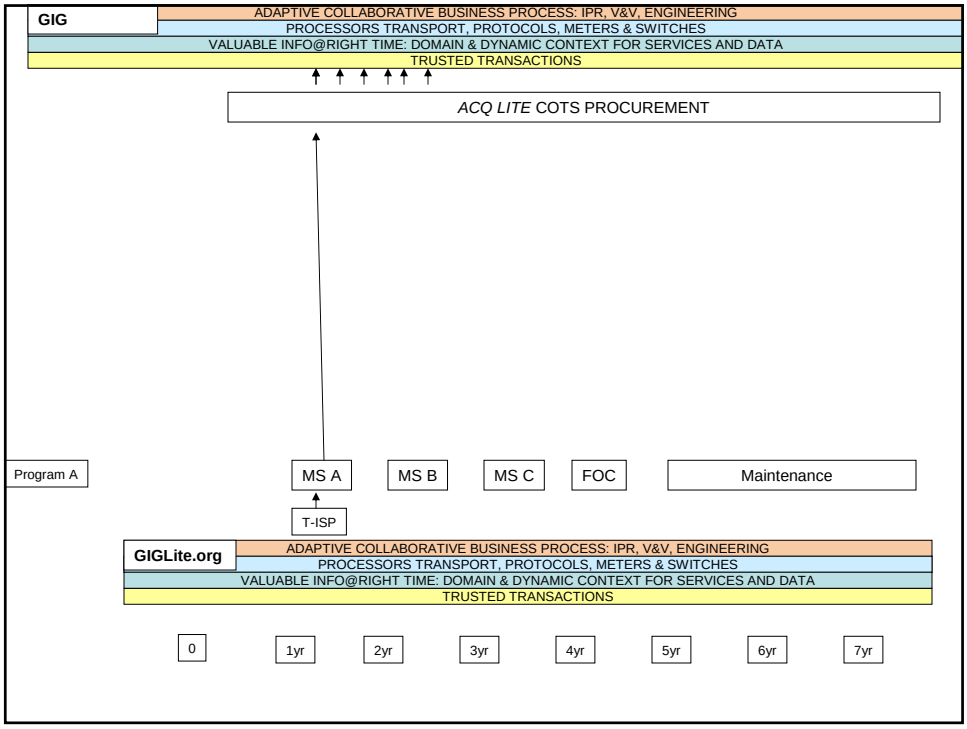
S&T → Demo → Engineer, V&V → Prototype → OPS Audit, Certify → Ref. Implementation → Bundle → Certified Product

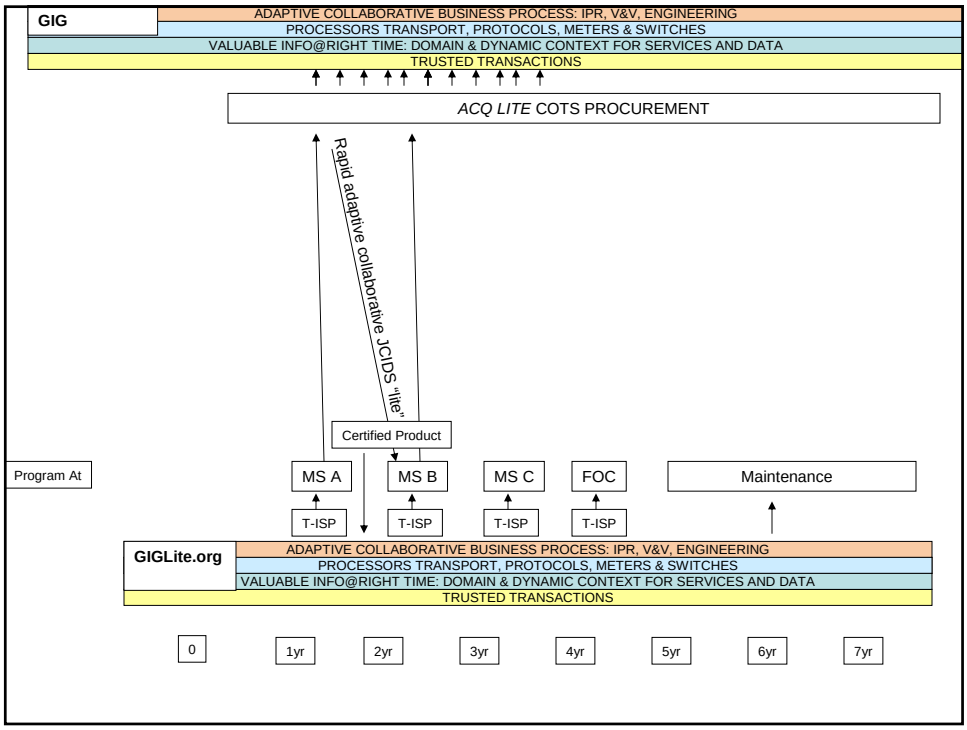
Program A | MS A | MS B | MS C | FOC | Maintenance

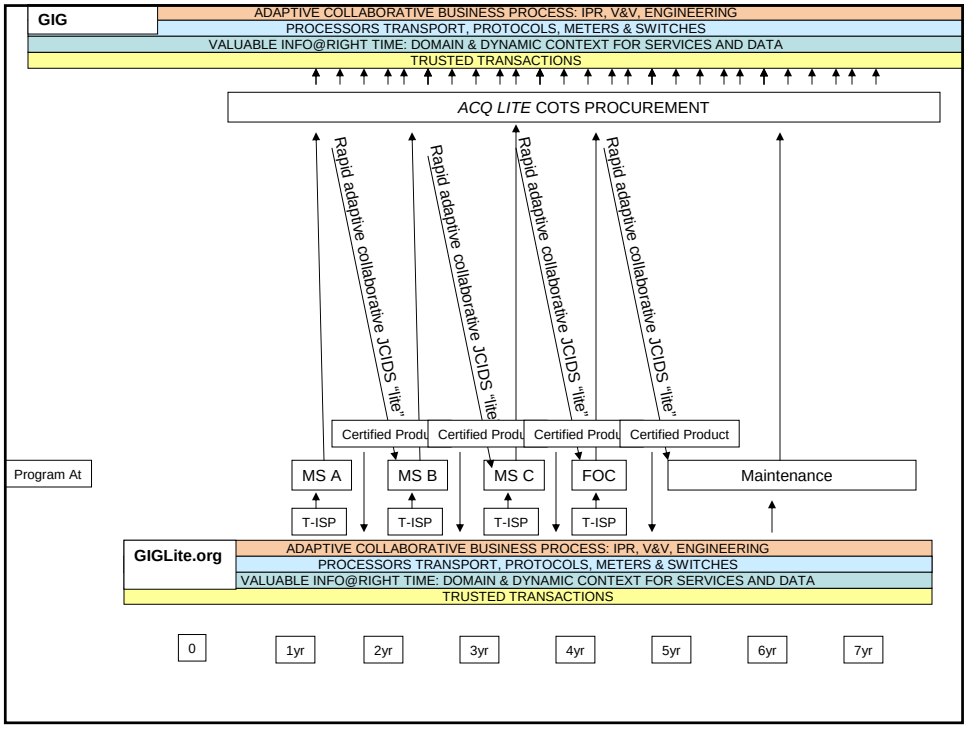
GIGLite.org

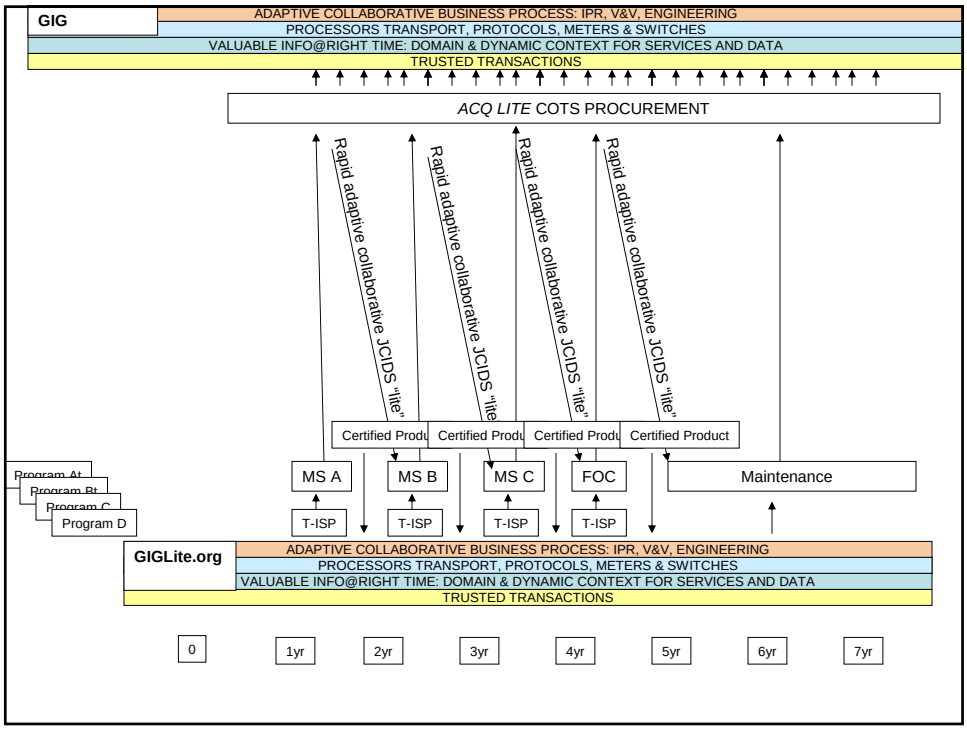
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS

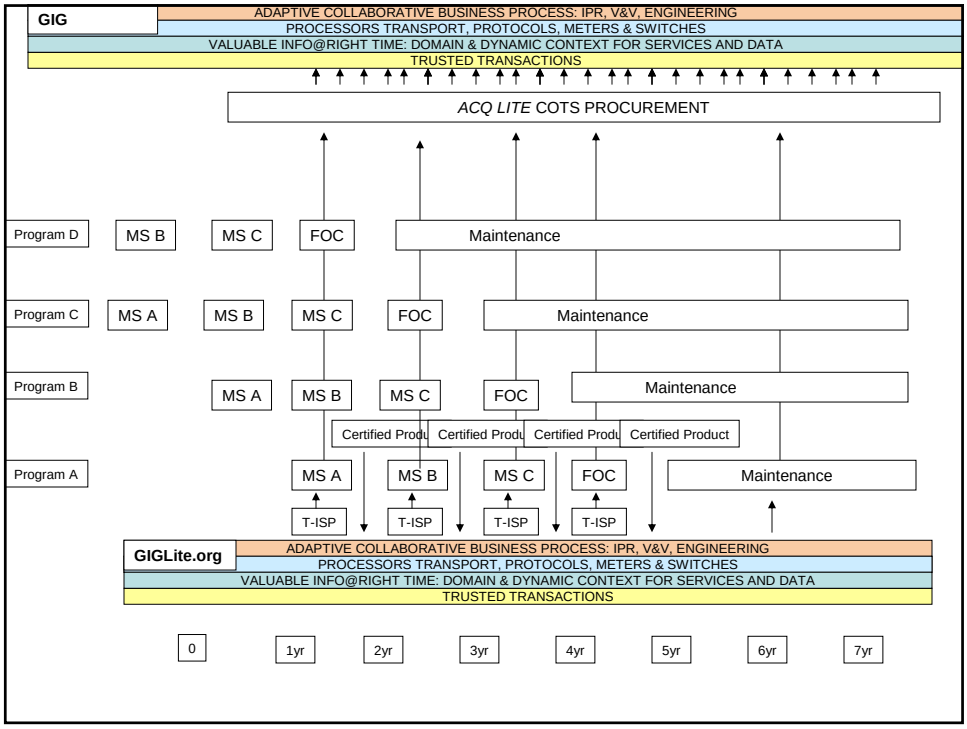
0 | 1yr | 2yr | 3yr | 4yr | 5yr | 6yr | 7yr


GIG
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS
ACQ LITE COTS PROCUREMENT
Program A
MS A
MS B
MS C
FOC
Maintenance
T-ISP
GIGLite.org
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS
0
1yr
2yr
3yr
4yr
5yr
6yr
7yr

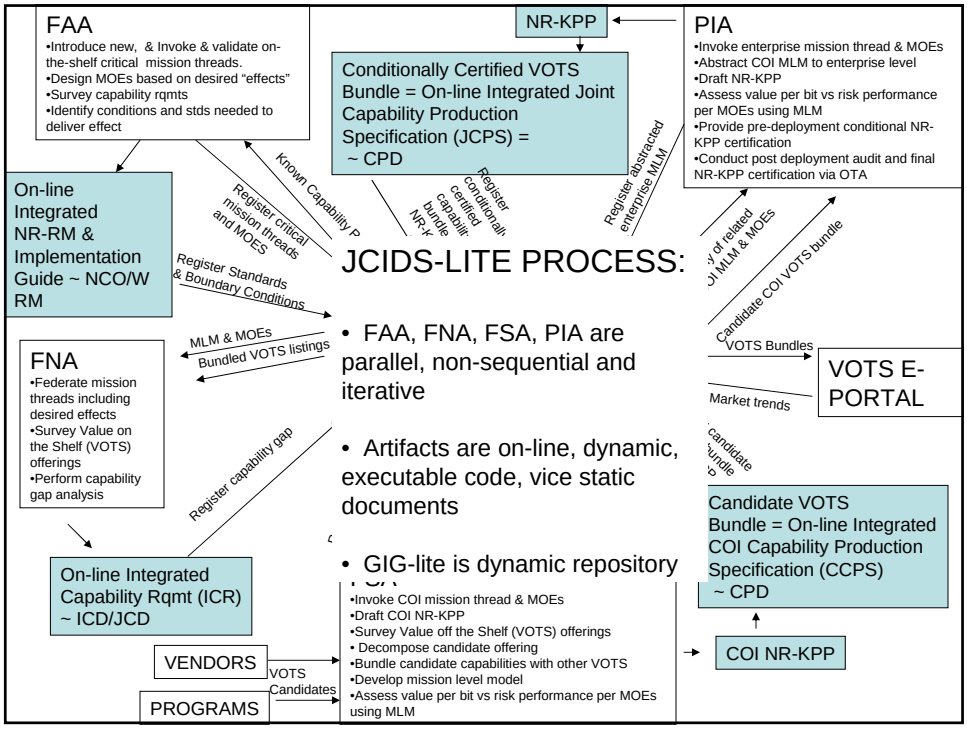

GIG
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS
ACQ LITE COTS PROCUREMENT
Rapid adaptive collaborative JCIDS "lite"
Certified Product
Program At
MS A
MS B
MS C
FOC
Maintenance
T-ISP
T-ISP
T-ISP
T-ISP
GIGLite.org
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS
0
1yr
2yr
3yr
4yr
5yr
6yr
7yr

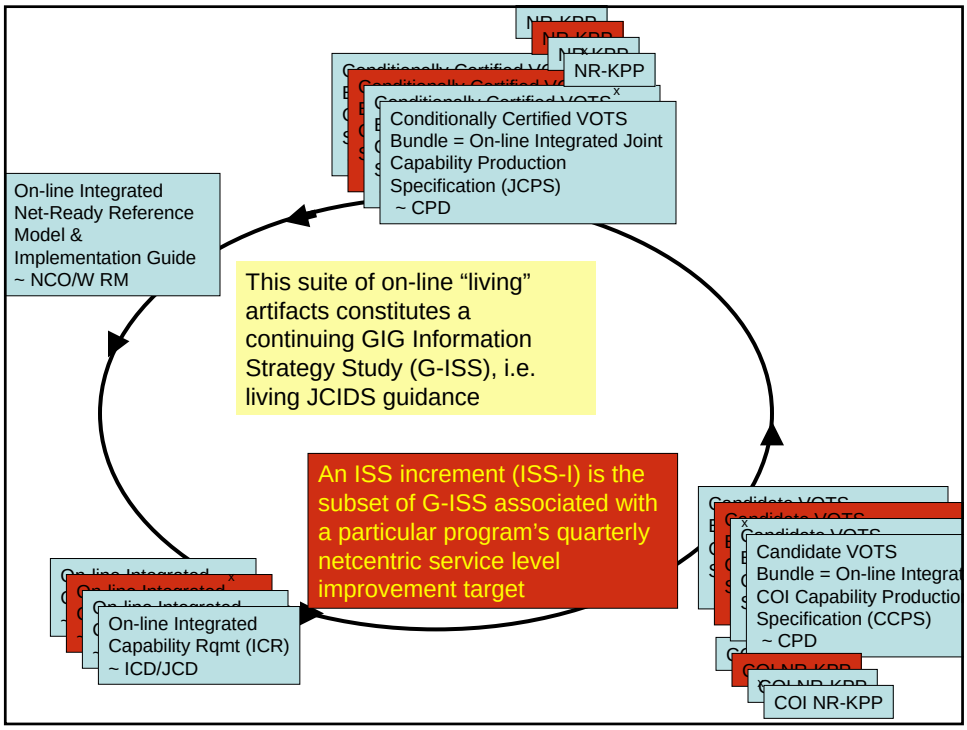

GIG
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS
ACQ LITE COTS PROCUREMENT
Rapid adaptive collaborative JCIDS "lite"
Rapid adaptive collaborative JCIDS "lite"
Rapid adaptive collaborative JCIDS "lite"
Rapid adaptive collaborative JCIDS "lite"
Certified Product
Certified Product
Certified Product
Certified Product
Program At
MS A
MS B
MS C
FOC
Maintenance
T-ISP
T-ISP
T-ISP
T-ISP
GIGLite.org
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS
0
1yr
2yr
3yr
4yr
5yr
6yr
7yr


GIG
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS
ACQ LITE COTS PROCUREMENT
Rapid adaptive collaborative JCIDS "lite"
Rapid adaptive collaborative JCIDS "lite"
Rapid adaptive collaborative JCIDS "lite"
Rapid adaptive collaborative JCIDS "lite"
Certified Product
Certified Product
Certified Product
Certified Product
Program A
Program B
Program C
Program D
MS A
MS B
MS C
FOC
Maintenance
T-ISP
T-ISP
T-ISP
T-ISP
GIGLite.org
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS
0
1yr
2yr
3yr
4yr
5yr
6yr
7yr


GIG
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS
ACQ LITE COTS PROCUREMENT
Program D
MS B
MS C
FOC
Maintenance
Program C
MS A
MS B
MS C
FOC
Maintenance
Program B
MS A
MS B
MS C
FOC
Maintenance
Certified Produ
Certified Produ
Certified Produ
Certified Product
Program A
MS A
MS B
MS C
FOC
Maintenance
T-ISP
T-ISP
T-ISP
T-ISP
GIGLite.org
ADAPTIVE COLLABORATIVE BUSINESS PROCESS: IPR, V&V, ENGINEERING
PROCESSORS TRANSPORT, PROTOCOLS, METERS & SWITCHES
VALUABLE INFO@RIGHT TIME: DOMAIN & DYNAMIC CONTEXT FOR SERVICES AND DATA
TRUSTED TRANSACTIONS
0
1yr
2yr
3yr
4yr
5yr
6yr
7yr

More Detail

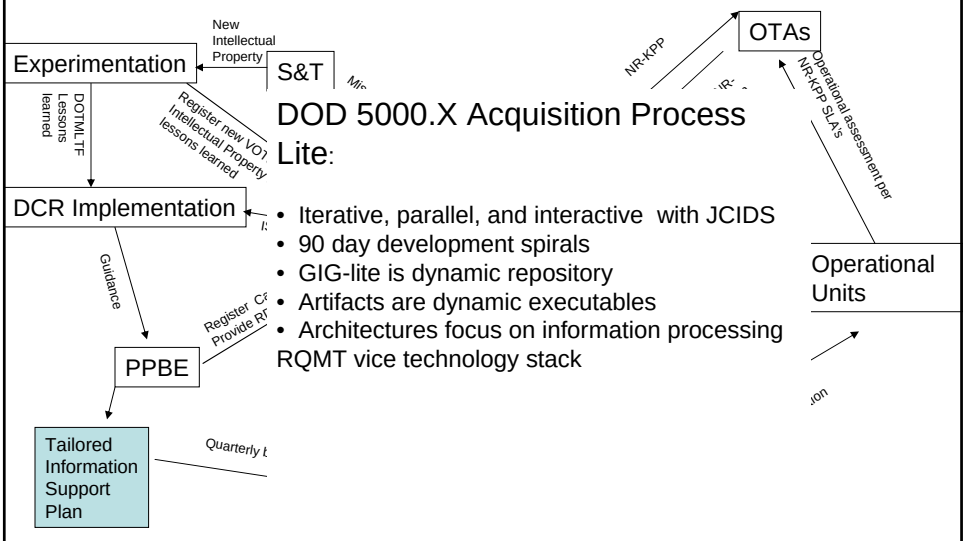

FAA
•Introduce new, & Invoke & validate on-the-shelf critical mission threads.
•Design MOEs based on desired "effects"
•Survey capability rqmts
•Identify conditions and stds needed to deliver effect
NR-KPP
Conditionally Certified VOTS Bundle = On-line Integrated Joint Capability Production Specification (JCPS) = ~ CPD
PIA
•Invoke enterprise mission thread & MOEs
•Abstract COI MLM to enterprise level
•Draft NR-KPP
•Assess value per bit vs risk performance per MOEs using MLM
•Provide pre-deployment conditional NR-KPP certification
•Conduct post deployment audit and final NR-KPP certification via OTA
On-line Integrated NR-RM & Implementation Guide ~ NCO/W RM
Known Capability P
Register critical mission threads and MOEs
Register conditionally certified capability bundle NR-K
Register abstracted enterprise MLM
Register Standards & Boundary Conditions
JCIDS-LITE PROCESS:
• FAA, FNA, FSA, PIA are parallel, non-sequential and iterative
• Artifacts are on-line, dynamic, executable code, vice static documents
• GIG-lite is dynamic repository
MLM & MOEs
Bundled VOTS listings
FNA
•Federate mission threads including desired effects
•Survey Value on the Shelf (VOTS) offerings
•Perform capability gap analysis
Candidate COI VOTS bundle
VOTS Bundles
VOTS E-PORTAL
Market trends
Register capability gap
Candidate VOTS Bundle = On-line Integrated COI Capability Production Specification (CCPS) ~ CPD
On-line Integrated Capability Rqmt (ICR) ~ ICD/JCD
•Invoke COI mission thread & MOEs
•Draft COI NR-KPP
•Survey Value off the Shelf (VOTS) offerings
• Decompose candidate offering
•Bundle candidate capabilities with other VOTS
•Develop mission level model
•Assess value per bit vs risk performance per MOEs using MLM
COI NR-KPP
VENDORS
PROGRAMS
VOTS Candidates

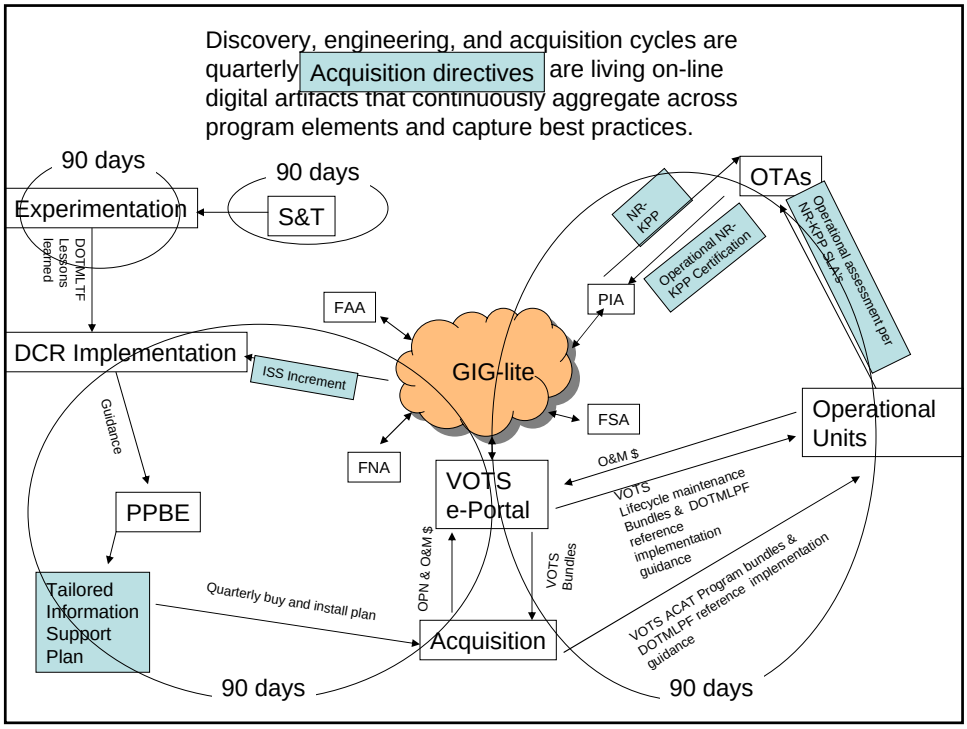

NR-KPP
Conditionally Certified VOTS Bundle = On-line Integrated Joint Capability Production Specification (JCPS) ~ CPD
On-line Integrated Net-Ready Reference Model & Implementation Guide ~ NCO/W RM
This suite of on-line "living" artifacts constitutes a continuing GIG Information Strategy Study (G-ISS), i.e. living JCIDS guidance
An ISS increment (ISS-I) is the subset of G-ISS associated with a particular program's quarterly netcentric service level improvement target
On-line Integrated Capability Rqmt (ICR) ~ ICD/JCD
Candidate VOTS Bundle = On-line Integrat COI Capability Productio Specification (CCPS) ~ CPD
COI NR-KPP

This suite of on-line “living” artifacts constitutes a continuing GIG Information Strategy Study (G-ISS), i.e. living JCIDS guidance

An ISS increment (ISS-I) is the subset of G-ISS associated with a particular program’s quarterly netcentric service level improvement target. ISS includes M&S-based developmental test & conditional certification

A program’s Tailored Information Support Plan (TISP) considers DOTMLPF Change Recommendation, fiscal facts of life, ISS-I, and provides a phased quarterly off-the-shelf procurement plan that is updated quarterly and specifies criteria for operational audit of NR-KPP SLA’s




Discovery, engineering, and acquisition cycles are quarterly
Acquisition directives
are living on-line digital artifacts that continuously aggregate across program elements and capture best practices.
90 days
Experimentation
90 days
S&T
DOTMLTF Lessons learned
DCR Implementation
ISS Increment
Guidance
PPBE
Tailored Information Support Plan
Quarterly buy and install plan
90 days
FAA
FNA
GIG-lite
FSA
PIA
NR-KPP
Operational NR-KPP Certification
OTAs
Operational assessment per NR-KPP SLAs
Operational Units
O&M $
VOTS e-Portal
VOTS Lifecycle maintenance Bundles & DOTMLPF reference implementation guidance
OPN & O&M $
VOTS Bundles
Acquisition
VOTS ACAT Program bundles & DOTMLPF reference implementation guidance
90 days